On the Finite Axiomatizability of Prenex R^1_2

Chris Pollett

Banff, Canada

Oct, 2011

Motivations

- S^1_2 is a bounded arithmetic theory whose $\hat{\Sigma}^b_1$-definable function correspond to polynomial time computable functions, the class FP.
- R^1_2 is a bounded arithmetic theory whose $\hat{\Sigma}^b_1$-definable function correspond to functions computable by polylog-depth polynomial-sized circuit families, the class FNC.
- Although not as great maybe as showing $\neq P$, proving a separation of R^1_2 from S^1_2 would imply new lower bounds on the provability of complexity problems. For instance, that R^1_2 can't prove $= -$ or that R^1_2 can't the collapse of polynomial hierarchy.
- Unfortunately, both these classes of functions and bounded arithmetic theories seem difficult to separate.
- However, if you look at the "prenex" version of R^1_2 you get a theory whose $\hat{\Sigma}^b_1$-consequences seem a fair bit weaker than FNC, so there seems to be some hope to separate this theory from S^1_2.
- This talk is about trying to come up with a good way to describe the $\hat{\Sigma}^b_1$-consequences of prenex R^1_2 that might lead to a separation result.

First-order Bounded Arithmetic

- The bounded arithmetic theories we will be looking at have BASIC axioms like:

$$y \le x \supset y \le S(x)$$
$$x + Sy = S(x + y)$$
$$\ldots$$

  for the symbols $0, S, +, \cdot, x\#y := 2^{|x||y|}, |x| :=$ length of x, $\dot{-}$, $\lfloor \frac{x}{2^i} \rfloor$, $\le$

- We add to this base theory $L^m IND_A$ induction axioms of the form:

$$A(0) \wedge \forall x < |t|_m [A(x) \supset A(S(x))] \supset A(|t|_m)$$

  Here t is a term made of compositions of variables and our function symbols and where we are using the definition $|x|_0 = x$, $|x|_m = ||x|_{m-1}|$.

String Manipulation, Collection/Replacement axioms

- Because we have $\lfloor \frac{x}{2^i} \rfloor$ in the language, it is possible to define as a term $\beta_a(i, w)$, the function which projects out the ith block of a bits out of w.
- We will also use later that we can define pairing and the function $BIT(j, w)$ as a terms.
- Besides induction another scheme known as BB_A or $REPL_A$:

  $$(\forall x \leq |s|)(\exists y \leq t(x))A(x, y) \supset (\exists w \leq bd(t^+, s))(\forall x \leq |s|)\beta_{|t^+|}(x, w) \leq t(x) \wedge A(x, \beta_{|t^+|}(x, w))$$

  will also be considered in this talk as it allows us to do a limited amount of quantifier exchange. Here t^+ is a monotone term derived from t. $bd(t^+, s)$ is a term used to a string of consisting of concatenating $|s|$ strings of length $|t^+|$.

Bounded Arithmetic Theories

- Σ_0^b (aka Π_0^b) are the bounded arithmetic formulas whose quantifiers are all of the form $(\forall x \leq |t|)$ or $(\exists x \leq |t|)$.
- For $i > 0$, Σ_i^b (resp. Π_i^b) are the closure of the Π_{i-1}^b (resp. Σ_{i-1}^b) formulas under conjunctions, disjunctions, $(\exists x \leq t)$ and $(\forall x \leq |t|)$ (for Π_i^b, $(\forall x \leq t)$ and $(\exists x \leq |t|)$).
- The prenex variant of the Σ_i^b formulas, the $\hat{\Sigma}_i$-formulas, look like:

$$(\exists x_1 \leq t_1) \cdots (Qx_i \leq t_i)(Qx_{i+1} \leq |t_{i+1}|)A$$

  where A is an open formula. So we have $i + 1$ alternations, innermost being length-bounded.
- A $\hat{\Pi}_i$-formula is defined similarly but with the outer quantifier being universal.
- T_2^i is the theory $BASIC+\Sigma_i^b$-IND.
  S_2^i is the theory $BASIC+\Sigma_i^b$-$LIND$.
  R_2^i is the theory $BASIC+\Sigma_i^b$-$LLIND$.

Prenex Theories

- It seems natural to ask if it makes any difference to define T_2^i, S_2^i, or R_2^i using $\hat{\Sigma}_i$-$L^m IND$ rather than Σ_i^b-$L^m IND$.
- For T_2^i and S_2^i it makes no difference as the prenex theory can prove $BB\Sigma_i^b$ and so can convert between prenex and non-prenex formulas. For R_2^i, it is not known.
- We denote the prenex version of R_2^i by $\hat{R}_2^i$.
- We write $\hat{T}_2^{i,\{|id|_m\}}$ for the theories $BASIC$+$\hat{\Sigma}_i$-$L^m IND$.

Definability

- Let Ψ be a class of formulas, we say a theory T can **Ψ-define a function** f if there is a Ψ-formula A_f such that

$$T \vdash \forall x \exists ! y A_f(x, y)$$

and

$$\mathbb{N} \vDash \forall x A_f(x, f(x))$$

Recapping + What's Known

- As we said earlier, the $\hat{\Sigma}_1$-definable function of S^1_2 and R^1_2 are (Buss) and FNC (Allen, Clote, Takeuti) respectively.
- Multifunction algebras for the $\hat{\Sigma}_1$-definable multifunctions of $\hat{R}^1_2$ and $\hat{T}_2^{1,\{|id|_m\}}$ are known from Pollett (2000).
- That paper also used a Johannsen-style block counting argument to show for $m \geq 4$ the multifunction algebra one gets cannot define $\lfloor \frac{x}{3} \rfloor$.
- Boughattas and Ressayre (2009) using a model theoretic technique then separated $\hat{T}_2^{1,\{|id|_3\}}$ from S^1_2.

One Possible Separation Approach...

- Jerabek (2006) showed S^1_2 was Σ^b_1-convervative over T^0_2.
- For $i \geq 1$, Pollett (1999) had a result that $T_2^{i,\{2^{p(||id||)}\}} \preceq_{\forall\hat{\Sigma}_{i+1}} R^{i+1}_2$.
- Here the $\{2^{p(||id||)}\}$ indicates the bound on induction.
- So it was natural to conjecture Jerabek's techniques could be used to show that $T_2^{0,\{2^{p(||id||)}\}} \preceq_{\forall\hat{\Sigma}_1} \hat{R}^1_2$.
- The hope would be then that some weaker notion of definability might then be used to separate $T_2^{0,\{2^{p(||id||)}\}}$ from T^0_2, and hence separating $\hat{R}^1_2$ from S^1_2.

... That doesn't seem to work.

- Pollett (2011) shows $T_2^{0,\{2^{p(||id||)}\}}$, again by a block counting argument, can't define $\lfloor \frac{x}{3} \rfloor$.
- It is unknown if $\hat{R}_2^1$ can define $\lfloor \frac{x}{3} \rfloor$. Certainly, R_2^1, which can define all functions in *FNC*, can.
- However, if you look take an $T_2^{0,\{2^{p(||id||)}\}}$ induction axiom and prenexify it, it has an outer existential that is of size $2^{p(||id||)}$ which is too small to be able to express a string that codes the steps of a computation of the kind of functions $\hat{R}_2^1$ can $\hat{\Sigma}_1$-define. So it is at least unlikely that $T_2^{0,\{2^{p(||id||)}\}}$ is conservative under $\hat{R}_2^1$.
- Pollett (2011) formulates a messy variant of a comprehension axiom called $open_{\{||id||\}}$-*COMP* (will describe in a moment) which when added to *LIOpen* (*BASIC*+*open-LIND*) suffice to carry out Jerabek's method and give a $\hat{\Sigma}_1$-conservative subtheory of R_2^1.
- There were earlier $\hat{\Sigma}_1$ theories for the functions in . For example, *TNC* of Clote Takeuti and RSUV isomorphisms of *VNC* of Cook Nguyen. The point here was to be able to carry out a modified Jerabek's construction. A later hope was that this could be modified to $\hat{R}_2^1$ with the goal to come up with as simple and breakable an axiomatization of $\forall\hat{\Sigma}_1(\hat{R}_2^1)$ as possible.

A New Strategy on $\hat{R}^1_2$ and R^1_2 versus S^1_2

- The function algebra for the $\hat{\Sigma}_1$-definable functions of $\hat{R}^1_2$ consists of initial functions of the language, the functions $\mu i \leq |a| t(i, a, \vec{b}) = 0$ for some term in the language (use $\hat{\Pi}_0$-$LIND$ to get), closure under composition and under the following kinds of recursion:
  $$F(0, x) = g(x)$$
  $$F(n + 1, x) = min(h(n, x, F(n, x)), r(n, x))$$
  $$f(n, x) = F(||t(n, x)||, x)$$
- To get the $\hat{\Sigma}_1$-definable functions, FP, of S^1_2 switch $||\cdot||$ to $|\cdot|$. For R^1_2, one adds to this closure under another kind of recursion called CRN.
- Expressed as a function algebra it seems hard to do things like diagonalization to separate these algebras.
- So ideally we want to get a normal form for the functions in these classes.
- Even if we can't separate the classes, and hence the original theories, the normal form will at least tell us something about finite axiomatization in the theories.

Axiomatisations for $\forall\hat{\Sigma}_1(\hat{R}^1_2)$, $\forall\hat{\Sigma}_1(R^1_2)$, and $\forall\hat{\Sigma}_1(S^1_2)$

- We begin with *BASIC*. To this we add the following *BITMIN* axiom
  $(\exists i \leq |a|)LEASTON(i, a)$
  where $LEASTON(i, a)$ is:
  $$(\forall j < i)[(i < |a| \supset BIT(i, a) = 1 \wedge BIT(j, a) = 0) \wedge$$
  $$(i = |a| \supset (\forall k < |a|)BIT(k, a) = 0)].$$
- This axiom can be proven in $\hat{R}^1_2$ using $\hat{\Pi}_0$-*LIND*, on the other hand it give us the sharply bounded μ-operator for terms.
- Next we add for each term t a bounded dependent choice axiom, $BDC_{\ell,t}$
  $$(\exists w \leq bd(d, b))(\forall i < \ell(b))[\beta_{|d|}(0, w) = min(a, d) \wedge$$
  $$t > 0 \supset \beta_{|d|}(i + 1, w) = min(t(\beta_{|d|}(i, w), i, a, b, c) \dot{-} 1, d) \wedge$$
  $$t = 0 \supset LEASTON(\beta_{|d|}(i + 1, w), \beta_{|d|}(i, w))].$$
  where ℓ is $|x|$ if we want $\forall\hat{\Sigma}_1(S^1_2)$ or of the form $||x||^k$ if we want $\forall\hat{\Sigma}_1(\hat{R}^1_2)$.
- For $\forall\hat{\Sigma}_1(R^1_2)$ you need in addition to add to $BDC_{\ell,t}$ another clause to handle *CRN*.

Remarks

- These are $\forall\hat{\Sigma}_1$ axioms and can be proven in the theory they correspond to by a straightforward induction argument.
- Let $ChoiceStr_\ell(w, a, b, c, d)$ the formula inside the $(\exists w \leq bd(d, b))$ in a $BDC_{\ell,t}$. Let $f(x, z)$ be a function, we say $f(x, z)$ is *ℓ-choice defined* if

$$f(x, z) = y \Leftrightarrow (\exists w \leq bd(2^{|s|}, t))[ChoiceStr_\ell(w, x, t, z, 2^{|s|}) \wedge OUT_f(w, x, z) = y]$$

  for some terms t, s not involving w, and for some term OUT_f.
- To show the conservativity result, you need to show the class of $||\cdot||^k$- (resp. $|\cdot|$-)choice defined functions have the necessary closure properties to carry out a witnessing argument.
- This gives that the $\hat{\Sigma}_1$-definable functions of $\hat{R}^1_2$, R^1_2, S^1_2 are just projections of these kind of choice strings.
- The main difference in the above and my 2011 Archive paper is that there I was working with open formulas rather than terms. This meant I had to define in an inductive fashion the open-formulas that would be suitable for the computation of a choice string.
- The set-up above looks very promising for diagonalization provided we could come with a nice universal predicate for choice strings.

Finite Axiomatizations

- Pairing, etc can be defined as terms in our language and using this we can give an encoding for terms as numbers.
- You could imagine adding a parameter e and modify our $ChoiceStr_{\ell}$ so that instead of having

$$\beta_{|d|}(i+1, w) = min(t(\beta_{|d|}(i, w), i, a, b, c) \dot{-} 1, d)$$

  we say that after $\beta_{|d|}(i, w)$, w codes a string which computes the operations according to the term coded by e_t until we get to what would have been $\beta_{|d|}(i+1, w)$.
- Writing this down, one would get a single $\hat{\Sigma}_1$-formula $U(e_t, a, b, c, d)$ which for different codes e_t would imply $BDC_{|id|,t}$. This gives an alternative proof to Cook-Kolokolova (2003) that $\forall\hat{\Sigma}_1(S^1_2)$ is finitely axiomatized.
- In the case of $\hat{R}^1_2$ and R^1_2 you get a sequence of formulas $U_k(e_t, a, b, c, d)$ for different values of k in
  $|| \cdot ||^k$.

Conclusion

- I conjecture that the theory, which over the base theory has the axiom U_{k+1}, is strictly stronger than the theory with U_k. I.e., $\forall\hat{\Sigma}_1(\hat{R}^1_2)$ and $\forall\hat{\Sigma}_1(R^1_2)$ are not finitely axiomatised.
- For R^1_2 these formulas probably correspond to hard problems at various levels of the NC^k hierarchy, so are likely hard to separate.
- The d parameter in $U_k(e_t, a, b, c, d)$ would typically be of the form $2^{|x|^e}$ and bounds the intermediate terms occuring in the choice string computation. Since it depends on e we can't immediately do diagonalization.
- However, maybe in $\hat{R}^1_2$ there is some clever way to compress the intermediate steps (as they are just given by terms) to within some $2^{|x|^c}$ for fixed ??? I end my talk with that open problem.